6712-01

This document is scheduled to be published in the Federal Register on 05/31/2022 and available online at **federalregister.gov/d/2022-11691**, and on **govinfo.gov**

FEDERAL COMMUNICATIONS COMMISSION

[FR ID 89498]

Privacy Act of 1974; System of Records

AGENCY: Federal Communications Commission.

ACTION: Notice of a modified system of records.

SUMMARY: In this document, the Federal Communications Commission (FCC or Commission or Agency) is modifying a system of records, FCC/OSP-1, Broadband Dead Zone Report and Consumer Broadband Test, subject to the Privacy Act of 1974, as amended. This action is necessary to implement the Broadband Data Collection (BDC) program. The modified system, now known as FCC/OEA-6, Broadband Data Collection system of records (BDC system), will collect granular, detailed information on the availability and quality of service of fixed and mobile broadband Internet access service from service providers, as well as verified broadband availability data from other Federal agencies, from State, local, and Tribal governmental entities that are primarily responsible for mapping or tracking broadband service coverage, and from other third parties. The BDC will additionally give the FCC, industry, Federal, State, local and Tribal government entities, and consumers the tools they need to continuously refine and improve the accuracy of these new mapping data. A number of broadband deployment funding mechanisms will rely upon BDC data, including the Broadband Equity, Access, and Deployment (BEAD) program, administered by the Department of Commerce's National Telecommunications and Information Administration (NTIA), the FCC's 5G Fund for Rural America, and potentially other broadband infrastructure deployment funding programs.

DATES: In accordance with 5 U.S.C. 552a(e)(4) and (11), this notice is effective upon publication, subject to a 30-day period in which to comment on the routine uses, described below. Please submit any comments by [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: Send comments to Brendan McTaggart, Federal Communications Commission (FCC), 45 L Street, NE, Washington, D.C. 20554, or to privacy@fcc.gov.

FOR FURTHER INFORMATION CONTACT: Brendan McTaggart, (202) 418-1738, or privacy@fcc.gov (and to obtain a copy of the Narrative Statement and the Supplementary Document, which includes details of the modifications to this system of records).

SUPPLEMENTARY INFORMATION: As required by the Privacy Act of 1974, as amended, 5 U.S.C. 552a(e)(4) and (e)(11), this document sets forth notice of the proposed modification of a system of records maintained by the FCC. The FCC previously provided notice of the system of records FCC/OSP-1, Broadband Dead Zone Report and Consumer Broadband Test, by publication in the **Federal Register** on July 14, 2011 (76 FR 41497).

This notice serves to modify FCC/OSP–1 to reflect a change in the name of the system of records, make various necessary changes and updates, including clarification of the purpose of the system, format changes required by OMB Circular A–108 since its previous publication, the addition of five new routine uses and the revision of five existing routine uses, which in several instances entailed converting a single existing routine use into multiple revised routine uses. The substantive changes and modification to the previously published version of FCC/OSP–1 system of records include: (1) adding routine uses related to sharing information with (a) the public; (b) broadband service providers; (c) other Federal agencies; (d) State, local, and Tribal governmental entities; and (e) certain FCC contractors or grantees; (2) revising routines uses related to sharing information with other Federal agencies, both for purposes directly related to the Broadband Data Collection as well as for law enforcement and data breach mitigation purposes; (3) substantially updating the Purposes of the System, Categories of Individuals, Categories of Records, and Sources of Records sections to accurately describe the BDC system.

SYSTEM NAME AND NUMBER: FCC/OEA-6, Broadband Data Collection

SECURITY CLASSIFICATION: No information in the system is classified.

SYSTEM LOCATION: Office of Economics and Analytics (OEA), Federal Communications Commission (FCC), 45 L Street, NE, Washington, D.C. 20554.

SYSTEM MANAGER: Office of Economics and Analytics (OEA), Federal Communications Commission (FCC), 45 L Street, NE, Washington, D.C. 20554.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Broadband Data Improvement Act of 2008, Pub. L. No. 110-385, Stat. 4096 § 103(c)(1); American Reinvestment and Recovery Act of 2009 (ARRA), Pub. L. No. 111-5, 123 Stat. 115 (2009); Communications Act, 47 U.S.C. 154(i); Broadband Deployment Accuracy and Technological Availability Act (Broadband DATA Act), Pub. L. No. 116-130, § 806(b), 134 Stat. 228, 238 (2020), amended by Infrastructure Investment and Jobs Act, Pub. L. No. 117-58, § 60102(h)(2)(E)(ii), 135 Stat. 429, 1198 (2021) (codified at 47 U.S.C. § 646(b)).

PURPOSES OF THE SYSTEM: The BDC system will collect granular, detailed information on the availability and quality of service of fixed and mobile broadband Internet access service from service providers, as well as verified broadband availability data from other Federal agencies, from State, local, and Tribal governmental entities that are primarily responsible for mapping or tracking broadband service coverage, and from other third parties. As part of the functionality of this system, various stakeholders, including consumers, can provide information about the accuracy of these data through the submission of challenge data and crowdsourced data. Certain information is required to properly validate challenge data and crowdsourced data submitted by consumers and to adjudicate challenges. The Categories of Records section below describes the types of information that will be collected from individuals as part of the fixed broadband challenge and crowdsourcing processes, and the Fabric challenge process. Information will also be collected from individuals through mobile speed test apps – including not only the FCC's mobile speed test application (FCC Speed Test App), built by an FCC contractor, but also other FCC-approved, third-party applications (*see Broadband Data Task Force and Office of Engineering and Technology Announce Procedures for Third-Party Mobile*

Speed Test Applications Seeking Approval for Use in the FCC's Broadband Data Collection, WC Docket No. 19-195, ET Docket No. 22-152, Public Notice, DA-22-408 (OET Apr. 14, 2022)) – which will enable individuals to participate in the BDC mobile challenge process and crowdsourcing efforts. A Privacy Act Statement or privacy notice will appear at all points of information collection from consumers.

To that end, the BDC platform does the following:

(1) Collects and disseminates granular broadband service availability data (broadband maps) from both fixed and mobile broadband providers, as well as governmental entities and third parties;

(2) Ingests the Broadband Serviceable Location Fabric (a common dataset of all locations in the United States and its territories where fixed broadband internet access service can be installed, and which must serve as the foundation upon which all data relating to the availability of fixed broadband internet access service must be reported and overlaid);

(3) Enables the submission of data challenging the accuracy of the FCC's broadband coverage maps, the information submitted by internet service providers regarding broadband service availability and quality of service, and/or the information included in the Fabric; and

(4) Enables the submission of crowdsourced data regarding the deployment and availability of broadband internet access service so that it may be used to verify and supplement information submitted by service providers for potential inclusion in the coverage maps.

As part of their participation in the challenge processes and other BDC mechanisms, it is the responsibility of the individuals to ensure the completeness and accuracy of the contact information and other data being provided at the time it is submitted into the BDC system. For individuals using the FCC Speed Test App, or another FCC-approved, third-party speed test application, this responsibility is shared by the individual and the mobile application provider. Once information is ingested by the BDC system, data integrity is controlled through user access safeguards and annual data validation testing (i.e., contingency planning exercises).

Information will be provided by consumers to the BDC system as part of the challenge processes. As noted, there are three types of challenges that can be initiated through the BDC: Fixed Broadband Challenges, Mobile Broadband Challenges, and Broadband Serviceable Location Fabric Challenges.

Fixed Broadband Challenges:

Entities and individuals can challenge whether a fixed broadband provider makes broadband service available at a particular broadband serviceable location (BSL) identified through the Fabric. After a challenger provides contact information and a justification for the challenge into the BDC system via a web-based form, an official ticket is created, along with a unique ticket number. The FCC monitors the ticket throughout the challenge process and will adjudicate challenges as necessary. The BDC system will notify individual challengers about the status of their challenge once the challenge is resolved.

Mobile Broadband Challenges:

Entities or individuals have the ability to download the FCC Speed Test App, or another FCC-approved, third-party mobile speed test application, to provide actual measurements of mobile broadband speeds and other metrics. These applications are not incorporated into the BDC system of records. The mechanisms used by the BDC for the mobile challenge process collect the following data: the challenger's email address and phone number, and the device identification, TCP/IP, time, and geo-location data associated with the speed test. This information is necessary to properly analyze and adjudicate consumer-initiated challenges.

The data collected by the FCC Speed Test App are transmitted to a database managed by SamKnows, the vendor for the FCC Speed Test App. SamKnows periodically transmits mobile speed test data from the database to the BDC system via a data transmission initiated by an automated Application Programming Interface (API) process, and the BDC system will acknowledge receipt of the submission. For FCC-approved, third-party mobile speed test applications, the collected mobile speed test data should be transmitted, stored, and maintained in

the third-party app developer's data repository system after the completion of active test measurements. The third-party app developer will similarly transmit the mobile speed test data periodically to the BDC system via a data transmission initiated by an automated API process, and the BDC system will acknowledge receipt of the submission.

These mobile speed test data will be subject to validation checks and algorithms developed by the FCC's Office of Economics and Analytics (OEA) to confirm the validity of the challenge data submission. The BDC system will aggregate validated speed test data with other submissions to create a cognizable mobile challenge in an area. Once a valid challenge data submission has formed the basis of a cognizable mobile challenge, a message will be sent to the challenger providing an update on the status of the challenge. At the same time as the challenger is notified that a cognizable mobile challenge has been created, the BDC system will notify the challenged mobile broadband service provider of the challenged area and provide details regarding the substance of the cognizable challenge, including underlying speed test data and relevant information about the challenger as necessary to allow the mobile service provider to respond to the challenge.

Broadband Serviceable Location Fabric Challenges:

Stakeholders can submit challenges to the Fabric data. The FCC relies on the Fabric when ingesting and publishing fixed broadband availability data. After a challenger provides contact information, information about a location that the challenger believes is incorrect in or missing from the Fabric, and a justification for the challenge, the BDC system creates an official ticket, along with a unique ticket number. The challenge data and associated ticket number are stored in a database within the FCC's BDC system. The FCC monitors the ticket through resolution. Once resolved, the challenger will receive a message with the resolution and status update.

Submission of Crowdsourced Data:

Entities or individuals may submit information about the deployment and availability of broadband internet access service so that it may be used to verify and supplement information submitted by providers for potential inclusion in the coverage maps. Crowdsourced data filers will provide, among other things, personal contact information (e.g., name, address, phone number, and email), the location that is the subject of the filing, including the street address and/or coordinates of the location; and a certification that to the best of the filer's actual knowledge, information, and belief, all statements in the filing are true and correct. Additionally, parties submitting mobile crowdsourced data must include the metrics and meet the testing parameters required for other entities to submit on-the-ground data to the Commission (*see* 47 CFR § 1.7006(c)(1)(i)-(ii)), except that the data may include any combination of download speed and upload speed rather than both.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: The categories of individuals in this system include individuals who have an interest in or are otherwise connected to the BDC, including individuals who (either in their own capacity or as a representative of a business or governmental entity): (1) submit broadband availability data, in the case of broadband service providers; (2) submit verified availability data, in the case of Federal agencies, State, local or Tribal governmental entities primarily responsible for mapping or tracking broadband coverage, or other third parties; and (3) elect to participate in the BDC fixed challenge process, fixed crowdsourced data collection, and the Fabric challenge process (either in the submission of challenge or crowdsourced data or in the submission of data in rebuttal to challenges), as well as each person who uses either the FCC Speed Test App or other FCC-approved, third-party mobile speed test applications to participate in the BDC mobile challenge and crowdsourcing processes).

CATEGORIES OF RECORDS IN THE SYSTEM: The categories of records in this system include: first and last name, street address (when relevant), phone number(s), email address, and, for the mobile challenge and crowdsource processes, geolocation or geographic coordinates

(latitude and longitude) information, the timestamp reflecting when the test measurement data were transmitted to the app developer's servers, user ID (unique device or application installation identifier), IP/MAC address (including source IP address and port of the device, as measured by the server), and other mobile device information (e.g., make, model, operating system).

RECORD SOURCE CATEGORIES: The sources for the information in this system are individuals, governmental entities (including Federal, State, local, and Tribal governmental entities), businesses, other third parties, and other FCC systems.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES: In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed to authorized entities, as is determined to be relevant and necessary, outside the FCC as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

1. Public Access – Pursuant to the FCC's Third Report and Order implementing the Broadband Data Collection (FCC-21-20), records related to the location of a challenge that is submitted as part of the challenge process will be made public, at times in aggregate form, via the Commission's website, including the street address and/or geographic coordinates as relevant. Location-related records related to the crowdsourcing process will also be made public via the Commission's website. Non-location related records associated with the challenge or crowdsourcing process, such as names, phone numbers, email addresses, or mobile device information will not be posted on the website.
2. Fixed and Mobile Broadband Service Providers – As described in the Purpose section above, certain records will be shared with fixed and mobile broadband service providers in order to help resolve challenges and/or address conflicting coverage information.
3. NTIA – Records, including provider contact information, may be shared with the National Telecommunications and Information Administration (NTIA) for administration of the

Broadband Equity, Access, and Deployment (BEAD) program and for other broadband programs funded under the Infrastructure Investment and Jobs Acts or other legislation. Additionally, records may be shared with NTIA in response to its submission of verified broadband availability data.

4. Other Federal Agencies – Records, including provider contact information, may be shared with other Federal agencies, including the Department of Agriculture and the Department of Treasury to support broadband programs funded under the Infrastructure Investment and Jobs Act or other legislation. For example, the Broadband DATA Act requires the FCC to share broadband maps with other Federal agencies upon request, while the Infrastructure Investment and Jobs Act requires coordination with Treasury and other agencies on the Broadband Deployment Locations Map. Additionally, records may be shared with other Federal agencies in response to their submission of verified broadband availability data.
5. State, Local, and Tribal Governmental Entities – Records, including provider contact information, may be shared with State, local, and Tribal governmental entities for use in their own broadband infrastructure funding programs, such as funding made available through Section 9901 of the American Rescue Plan Act of 2021, as well as in response to their submission of verified broadband availability data.
6. Contract Services, Grants, or Cooperative Agreements – Records may be shared with FCC contractors, grantees, or volunteers who have been engaged to assist the FCC in the performance of a contract service, grant, cooperative agreement, or other activity related to this system of records and who need to have access to the records in order to perform their activity. Examples include, but are not limited to, sharing records with the developers of FCC-approved, third-party mobile speed test applications; with wireless engineering firms assisting with the mobile challenge process; with technical assistance firms supporting the BDC help center; with outside auditing firms assisting with audits.
7. FCC Enforcement Actions – When a record in this system involves an informal complaint

filed alleging a violation of FCC rules and regulations by an applicant, licensee, certified or regulated entity, or an unlicensed person or entity, the complaint may be provided to the alleged violator for a response. Where a complainant in filing his or her complaint explicitly requests confidentiality of his or her name from public disclosure, the Commission will endeavor to protect such information from public disclosure. Complaints that contain requests for confidentiality may be dismissed if the Commission determines that the request impedes the Commission's ability to investigate and/or resolve the complaint.

8. Congressional Inquiries – To provide information to a Congressional office from the record of an individual in response to an inquiry from that Congressional office made at the request of that individual.
9. Government-Wide Program Management and Oversight – To the Department of Justice (DOJ) to obtain that department's advice regarding disclosure obligations under the Freedom of Information Act (FOIA); or the Office of Management and Budget (OMB) to obtain that office's advice regarding obligations under the Privacy Act.
10. Law Enforcement and Investigation – To disclose pertinent information to appropriate Federal, State, or local agencies, authorities, and officials responsible for investigating, prosecuting, enforcing, or implementing a statute, rule, regulation, or order, where the FCC becomes aware of an indication of a violation or potential violation of a civil or criminal statute, law, regulation, or order.
11. Litigation – To disclose records to the Department of Justice (DOJ) when: (a) the FCC or any component thereof; (b) any employee of the FCC in his or her official capacity; (c) any employee of the FCC in his or her individual capacity where the DOJ or the FCC has agreed to represent the employee; or (d) the United States Government is a party to litigation or has an interest in such litigation, and by careful review, the FCC determines that the records are both relevant and necessary to the litigation, and the use of such records by the Department of Justice is for a purpose that is compatible with the purpose for which the FCC collected

the records.

12. Adjudication – To disclose records in a proceeding before a court or adjudicative body, when: (a) the FCC or any component thereof; or (b) any employee of the FCC in his or her official capacity; or (c) any employee of the FCC in his or her individual capacity; or (d) the United States Government, is a party to litigation or has an interest in such litigation, and by careful review, the FCC determines that the records are both relevant and necessary to the litigation, and that the use of such records is for a purpose that is compatible with the purpose for which the agency collected the records.
13. Breach Notification – To appropriate agencies, entities, and persons when: (a) the Commission suspects or has confirmed that there has been a breach of the system of records; (b) the Commission has determined that as a result of the suspected or confirmed compromise there is a risk of harm to individuals, the Commission (including its information systems, programs, and operations), the Federal Government, or national security; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Commission's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.
14. Assistance to Federal Agencies and Entities Related to Breaches – To another Federal agency or Federal entity when the Commission determines that information from this system is reasonably necessary to assist the recipient agency or entity in: (a) responding to a suspected or confirmed breach, or (b) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, program, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.
15. Prevention of Fraud, Waste, and Abuse Disclosure – To Federal agencies, non-Federal entities, their employees, and agents (including contractors, their agents or employees; employees or contractors of the agents or designated agents); or contractors, their employees

or agents with whom the FCC has a contract, service agreement, cooperative agreement, or computer matching agreement for the purpose of: (1) detection, prevention, and recovery of improper payments; (2) detection and prevention of fraud, waste, and abuse in Federal programs administered by a Federal agency or non-Federal entity; (3) detection of fraud, waste, and abuse by individuals in their operations and programs, but only to the extent that the information shared is necessary and relevant to verify pre-award and prepayment requirements prior to the release of Federal funds, prevent and recover improper payments for services rendered under programs of the FCC or of those Federal agencies and non-Federal entities to which the FCC provides information under this routine use.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: This is an electronic system of records that resides on the FCC's network or on an FCC vendor's network.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Records in this system of records can be retrieved by any category field, e.g., first name or email address.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: The information in this system is maintained and disposed of in accordance with the National Archives and Records Administration (NARA) General Records Schedule 6.5, Item 020 (DAA-GRS-2017-0002-0002).

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: Before a service provider receives access to crowdsourced or challenge data, it will be required, within the BDC platform, to acknowledge that it will use personally identifiable information that it receives for the sole purpose of responding to a challenge and that it will protect and keep private all such personally identifiable information.

The FCC protects its information resources with a dynamic set of security measures. Some of these measures (e.g., network firewalls, physical security) protect the entire FCC enterprise, while other measures (e.g., user access restrictions, encryption) are applied to specific information systems. Following the risk-based policy established in the Federal Information

Modernization Act (FISMA), the FCC applies more security measures (also known as security "controls") to information systems that present higher operational risks. Consistent with this policy, the FCC applies specific security controls to systems that collect and process Privacy Act records. A comprehensive list of the security and privacy controls the FCC may apply to its information systems can be found in National Institute of Standards and Technology (NIST) Special Publication (SP) No. 800-53, Revision 5. Finally, the BDC resides within the FCC instance of AWS, which is FedRAMP accredited, and any customer responsibility controls are addressed through NIST SP No. 800-53.

The electronic records, files, and data are stored within FCC or a vendor's accreditation boundaries and maintained in a database housed in the FCC's or vendor's computer network databases. Access to the electronic files is restricted to authorized employees and contractors; and to IT staff, contractors, and vendors who maintain the IT networks and services. Other employees and contractors may be granted access solely on a need-to-know basis. The electronic files and records are protected by the FCC and third-party privacy safeguards, a comprehensive and dynamic set of IT safety and security protocols and features that are designed to meet all Federal privacy standards, including those required by the Federal Information Security Modernization Act of 2014 (FISMA), the Office of Management and Budget (OMB), and the National Institute of Standards and Technology (NIST).

RECORD ACCESS PROCEDURES: Individuals wishing to request access to and/or amendment of records about themselves should follow the Notification Procedure below.

CONTESTING RECORD PROCEDURES: Individuals wishing to request access to and/or amendment of records about themselves should follow the Notification Procedures below.

NOTIFICATION PROCEDURES: Individuals wishing to determine whether this system of records contains information about themselves may do so by emailing privacy@fcc.gov. Individuals requesting access must also comply with the FCC's Privacy Act regulations

regarding verification of identity to gain access to records as required under 47 CFR part 0, subpart E.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: None.

HISTORY: 76 FR 41497 (July 14, 2011)

FEDERAL COMMUNICATIONS COMMISSION.

Marlene Dortch,

Secretary.

[FR Doc. 2022-11691 Filed: 5/27/2022 8:45 am; Publication Date: 5/31/2022]